NO. 17-17351

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ENIGMA SOFTWARE GROUP USA, LLC,

PLAINTIFF- APPELLANT,

V.

MALWAREBYTES, INC.,

DEFENDANT-APPELLEE.

On Appeal from the United States District Court
for the Northern District of California
No. 5:17-cv-02915-EJD
Hon. Edward J. Davila, District Judge, Presiding

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND CAUCE NORTH AMERICA, INC. IN SUPPORT OF DEFENDANT-APPELLEE MALWAREBYTES, INC.'S PETITION FOR PANEL REHEARING AND REHEARING EN BANC

Sophia Cope
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
sophia@eff.org
amackey@eff.org
(415) 436-9333

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* Electronic Frontier Foundation and CAUCE North America, Inc. state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: November 6, 2019

By: /s/ *Sophia Cope*
Sophia Cope

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

STATEMENT OF INTEREST[1]

Amicus Curiae Electronic Frontier Foundation (EFF) is a member-supported, non-profit civil liberties organization that works to protect free speech, privacy, security, and innovation in the digital world. Founded in 1990, EFF has over 30,000 members. EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law to the Internet and other technologies. EFF has litigated or otherwise participated in a broad range of intermediary liability cases.[2]

Amicus Curiae CAUCE North America, Inc., the Coalition Against Unsolicited Commercial Email, is a non-profit all-volunteer consumer advocacy organization. It actively advocates on behalf of consumers to governments, legislators, law enforcement agencies, and industry associations about matters related to the blended threat of spam, viruses and spyware, and engages in user and industry outreach and education about this threat.[3]

---

[1] No counsel for a party authored this brief in whole or in part, and no person other than *amici* or their counsel has made any monetary contributions intended to fund the preparation or submission of this brief. The parties have consented to the filing of this brief.

[2] *See generally CDA 230*, EFF, https://www.eff.org/issues/cda230.

[3] In 2008, *amici* EFF and CAUCE signed onto an *amicus* brief arguing that Section 230(c)(2)(B) should be read to include an implicit "good faith" exception. *See Brief Amici Curiae of the Anti-Spyware Coalition, et al., Zango, Inc. v. Kaspersky Lab, Inc.*, No. 07-35800 (9th Cir.), pp. 23-25, https://cdt.org/files/2012/03/20080505amicus.pdf. Given events in the intervening

INTRODUCTION

Amici write in support of Defendant-Appellee Malwarebytes' Petition for Panel Rehearing and Rehearing En Banc of the panel decision in *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 938 F.3d 1026 (9th Cir. 2019). *See* ECF No. 56 (Oct. 28, 2019). Rehearing en banc is "necessary to secure or maintain uniformity of the court's decisions," Fed. R. App. P. 35(a)(1), particularly this Court's decision in *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir.

---

decade, *amici* today firmly believe that reading an implicit good faith exception into Section 230(c)(2)(B) is no longer good policy or necessary, and that a stricter statutory reading is more appropriate. First, the fallout from Congress' passage of the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), Pub. L. 115-164 (2018) in 2018 strongly supports the conclusion that new exceptions to Section 230 immunities should not be created; doing so results in real chilling effects, causing providers to take actions that harm Internet users. *See infra* Part II.C. Second, EFF has expanded its work to include the development of free privacy-enhancing tools for Internet users, and thus directly benefits from the immunity provided by Section 230(c)(2)(B). *See infra* Part III. Third, the two examples given in the *Zango* brief of anti-competitive or fraudulent filtering should be viewed in a modern context. The first example involved a broadband access provider that also provides cable TV video services blocking online video sites. *Amici* today believe this example would be best addressed by "net neutrality" rules, which EFF has been vigorously advocating for in recent years. *See Net Neutrality*, EFF, https://www.eff.org/issues/net-neutrality. The second example involved a filtering tool provider that distributes software that causes harassing advertisements to pop up on users' screens, and then offers to block the harassing ads for a fee. Such a practice might be, for example, prosecutable under the federal criminal statute for wire fraud. *See* 18 U.S.C. § 1343. Thus, given Section 230's carve-out for federal criminal laws, *see* 47 U.S.C. § 230(e)(1), truly culpable online entities can be targeted without relying on new exceptions to Section 230. *See, e.g.*, Stop Advertising Victims of Exploitation Act (SAVE Act), § 118, Pub. L. 114-22 (2015) (amending federal criminal sex trafficking statute, 18 U.S.C. § 1591, to include advertising).

2009); and this "proceeding involves a question of exceptional importance," Fed. R. App. P. 35(a)(2).

Amici represent the interests of Internet users and support Malwarebytes' petition because the *Enigma* panel's ruling will discourage the development of effective tools that allow users to customize their experiences online. Reading Section 230(c)(2)(B) (47 U.S.C. § 230(c)(2)(B)) to provide unequivocal protection to the providers of filtering tools, which the *Enigma* panel failed to do, is consistent with the plain meaning of the statute and congressional policy goals, and ultimately best empowers Internet users by incentivizing the development of robust and diverse filtering tools.

Filtering tools give Internet users choices. People use filtering tools to directly protect themselves and to craft the online experiences that comport with their values, by screening out spyware, adware, or other forms of malware, spam, or content they deem inappropriate or offensive. Platforms use filtering tools for the same reasons, enabling them to create diverse places for people online.

Amicus EFF also supports rehearing because it directly benefits from a plain reading of Section 230(c)(2)(B), as its public interest technologists have developed a free tool, called Privacy Badger, that stops advertisers and other third-party trackers from secretly tracking users as they browse the web. EFF's ability to

continue providing free privacy-enhancing tools to Internet users will be seriously threatened if the panel's incorrect interpretation of Section 230(c)(2)(B) stands.

Finally, *amicus* EFF supports rehearing because ensuring that Section 230(c)(2)(B) unequivocally protects filtering tool providers encourages those providers to block harmful software that is used to perpetuate domestic violence and harassment. EFF is working to eradicate this so-called "stalkerware," and that goal is more likely to be achieved when filtering tool providers have the unqualified Section 230(c)(2)(B) immunity that Congress intended.

ARGUMENT

I. The *Enigma* Panel's Decision Is Inconsistent with *Zango*, and the Plain Language of Section 230(c)(2)(B) Does Not Include an Anti-Competitive or Good Faith Exception

The *Enigma* panel rejected Defendant-Appellee Malwarebytes' motion to dismiss the complaint, erroneously holding that there is an exception to the immunity provided by Section 230(c)(2)(B) where the plaintiff alleges that a developer of a filtering tool had an "anticompetitive animus" in blocking the plaintiff's product. *See Enigma Software Group USA, LLC*, 938 F.3d at 1030.

The *Enigma* panel's decision is inconsistent with the *Zango* decision. *See* Fed. R. App. P. 35(a)(1). The *Enigma* panel in effect read a general "good faith" exception into Section 230(c)(2)(B), which does not exist within the plain meaning of the statutory language and which Congress did not intend to implicitly include.

In contrast to the *Enigma* panel's decision, the *Zango* majority did not read any exception into Section 230(c)(2)(B). Section 230(c)(2)(B) provides immunity for the blocking of material described in Section 230(c)(2)(A), which includes material that is "objectionable." 47 U.S.C. § 230(c)(2)(A) & (B). This Court was correct to hold in *Zango* that a provider of a filtering tool that blocks content or products that "the *provider or user* considers obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable is protected from liability" by Section 230(c)(2)(B). *See Zango, Inc.*, 568 F.3d at 1177-78 (emphasis added). Thus, the *Zango* Court explicitly held that the filtering tool provider *itself* may be the one who subjectively decides what content or products count as "objectionable" per Section 230(c)(2)(A) and therefore may be subject to blocking that is immunized under Section 230(c)(2)(B). *Zango, Inc.*, 568 F.3d at 1173.

Yet the *Enigma* panel substituted its own determination of what counts as "objectionable" material per Section 230(c)(2)(A), rather than deferring to what a filtering tool provider has decided to block. The *Enigma* panel thus erroneously held that Malwarebytes' blocking of a competitor's product allegedly based on an "anticompetitive animus" makes the blocked software not "objectionable" material and thus does "not fall within any category listed in [Section 230(c)(2)(A)] and the [Section 230(c)(2)(B)] immunity [does] not apply." *See Enigma Software Group USA, LLC*, 938 F.3d at 1037.

By voiding statutory immunity when blocking allegedly occurred for an anti-competitive purpose, the *Enigma* panel effectively created a general "good faith" exception to the immunity granted to providers of filtering tools by Section 230(c)(2)(B). Indeed, the *Enigma* panel cited Judge Fisher's concurrence in *Zango*, *Enigma Software Group USA, LLC*, 938 F.3d at 1036, and Judge Fisher endorsed a "good faith limitation" to Section 230(c)(2)(B)'s immunity, *Zango, Inc.*, 568 F.3d at 1179 (Fisher, J., concurring).

However, the *Enigma* panel's reading of a good faith exception into Section 230(c)(2)(B) is contrary to the plain language of the subsection specifically and the statute as a whole. While Section 230(c)(2)(A) does have an express good faith limitation, Section 230(c)(2)(B) does not. *See* 47 U.S.C. § 230(c)(2)(A) & (B). The *Zango* Court noted that Section 230(c)(2)(B) has only "one constraint" and good faith is not it. *Zango, Inc.*, 568 F.3d at 1177. Moreover, the rules of statutory interpretation counsel against reading such an exception into Section 230(c)(2)(B). "[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello v. United States*, 464 U.S. 16, 23 (1983) (internal quotations and citation omitted). *See also Prager Univ. v. Google LLC*, No. 19-CV-340667 (Cal. Super. Ct. Santa Clara

Cty. Oct. 25, 2019) (tentative ruling) ("The Court … disagrees with the majority in *Enigma*, who ignore the plain language of the statute….").

II. Reading Any Exception Into Section 230(c)(2)(B) Immunity Harms Internet Users

Reading any exception into Section 230(c)(2)(B) ultimately harms Internet users. It may be true, as the *Enigma* panel stated, that "[u]sers would not reasonably anticipate providers blocking valuable online content in order to stifle competition." *Enigma Software Group USA, LLC*, 938 F.3d at 1036. However, creating an anti-competitive or good faith exception to Section 230(c)(2)(B) immunity, or any exception for that matter, *on balance* harms Internet users more than when a particular filtering tool provider blocks a competitor's product.[4] This is because the *Enigma* panel's decision—by exposing filtering tool providers to new legal liability, as well as the costs and burdens of litigation—is likely to lead to Internet users having *less robust and fewer* filtering tools to choose from, disempowering them (and the platforms they use) from fashioning the online experiences that reflect their values.

[4] In this case, as the *Enigma* panel suggested, if an Internet user already has Malwarebytes' filtering tool installed, and the user then attempts to download Enigma's products, the user is given a warning but may actually continue with the download. *Enigma Software Group USA, LLC*, 938 F.3d at 1033.

A. The *Enigma* Panel's Decision Will Chill the Development of Online Filtering Tools

The *Enigma* panel's decision creates legal uncertainty for filtering tool providers that, in turn, promises to create a chilling effect to the detriment of Internet users. Should the decision stand, filtering tool providers will seek to minimize their legal exposure by creating weaker, less effective filtering tools for fear of sweeping in competitors—or otherwise doing something that could lead to allegations of acting in "bad faith." Additionally, some would-be entrepreneurs might not even take the chance on entering the filtering tool market in the first place.

This chilling effect flows not just from the fear of being held legally liable for a variety of causes of action, but also from the fear of having to face costly and burdensome litigation. Small filtering tool companies, in particular, may have difficulty shouldering the costs of litigation, in addition to ultimate liability. In this case, Enigma's allegations of "anticompetitive animus" on the part of Malwarebytes were sufficient to defeat a motion to dismiss. *Enigma Software Group USA, LLC*, 938 F.3d at 1030. This means that a filtering tool provider may, in fact, have acted in good faith by blocking a competitor, but it may be sued anyway via a plausibly alleged complaint, *see Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and would be required to defend itself through discovery, then summary judgment or trial—which are, of course, very long and costly legal proceedings.

Yet Congress intended Section 230 to provide immunities from suit as well as liability. *See* 47 U.S.C. § 230(e)(3) ("[n]o cause of action may be brought and no liability may be imposed"); *Fair Housing Counsel of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1174 (9th Cir. 2008) (en banc) (holding that Section 230 cases "must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites"); *Hassell v. Bird*, 5 Cal. 5th 522, 544 (2018); *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 (4th Cir. 2009).

B. Online Filtering Tools May Inadvertently Flag False Positives

The risk of losing a motion to dismiss despite having acted in good faith is real given how online filtering tools function. Whether they screen out spyware, adware, or other forms of malware, spam, or unwanted content, online filtering tools operate by using two main methodologies. One involves the creation of block lists of known bad software, websites, or content, also called a "signature-based analysis." The other involves the use of heuristics or rules-based filtering.[5] As the

[5] *See* Karen Scarfone & Peter Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Special Publication 800-94, § 8.3.2, Nat'l Inst. of Standards & Tech. (NIST), U.S. Dept. of Commerce (Feb. 2007) ("Both antivirus and antispyware products detect threats primarily through signature-based analysis. To identify previously unknown threats, they also use heuristic techniques that examine activity for certain suspicious characteristics."), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Enigma panel explained, Malwarebytes similarly uses "criteria" to flag potentially problematic software. *Enigma Software Group USA, LLC*, 938 F.3d at 1033.

Thus, the first methodology implies deliberate action or an intent to block by the filtering tool provider. The second methodology, by contrast, may result in a competitor being flagged by the filtering tool, but this fact alone does not *prove* an allegation of an anti-competitive purpose. The flagging of a competitor may have been done inadvertently, for reasons unrelated to the fact that the company is a competitor.[6] Thus, false positives are possible, yet a filtering tool provider may be sued, lose a motion to dismiss, and be forced to carry on through discovery and a ruling on the merits in order to prove it acted in good faith.

C. The FOSTA Fallout Illustrates the Risks of Creating New Exceptions to Section 230

The chilling effect that results from weakening any of Section 230's immunities is best illustrated by the far-reaching and harmful consequences to user speech that followed Congress' passage of the Allow States and Victims to Fight

[6] *See* Lenny Zeltser, *How antivirus software works; Virus detection techniques*, SearchSecurity.com (Oct. 2011) ("The biggest downside of heuristics is it can inadvertently flag legitimate files as malicious."), https://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques.

Online Sex Trafficking Act (FOSTA) in 2018.[7] FOSTA, in part, amended Section 230 to weaken the statutory protection provided by Section 230(c)(1) to platforms that host user-generated content in an effort to combat sex trafficking. *See* § 4, Pub. L. 115-164 (2018); 47 U.S.C. § 230(e)(5).

As a result, many platforms that hosted user-generated "adult" content immediately sought to mitigate their legal exposure under the new law to the detriment of Internet users. Although FOSTA was ostensibly intended to curb unlawful content and related behavior, its silencing effect went far beyond unlawful speech. Craigslist, the online classified ads site, for example, shut down its personals section, a loss to people who used the section for lawful purposes.[8] Pounced, a niche dating site, shut down entirely because of FOSTA.[9] Other platforms appeared to

[7] *See* Jason Kelley and Aaron Mackey, *Don't Repeat FOSTA's Mistakes*, EFF (March 29, 2019), https://www.eff.org/deeplinks/2019/03/dont-repeat-fostas-mistakes.

[8] Craigslist, *About FOSTA*, https://www.craigslist.org/about/FOSTA.

[9] Samantha Cole, *Furry Dating Site Shuts Down Because of FOSTA*, Vice (April 2, 2018), https://www.vice.com/en_us/article/8xk8m4/furry-dating-site-pounced-is-down-fosta-sesta.

react to the passage of FOSTA: Tumblr, the blogging site, banned all adult content,[10] while Facebook created a new "sexual solicitation" policy.[11]

The Fourth Circuit predicted the fallout that would occur with any weakening of Section 230(c)(1)'s immunity against liability for platforms that host user-generated content: "Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted." *Zeran v. AOL*, 129 F.3d 327, 331 (4th Cir. 1997).

In light of online platforms' response to FOSTA, it is more than likely that filtering tool providers will take similar steps to limit their legal exposure should the *Enigma* panel decision stand. But instead of taking down more user-generated content as platforms did in response to FOSTA, filtering tool providers will be reluctant to block certain software or content, as those decisions may later be alleged to have been the result of "anticompetitive animus" or "bad faith." This will dampen the market for innovative filtering technologies and may ultimately make users less safe online.

---

[10] Shannon Liao, *Tumblr will ban all adult content on December 17th*, The Verge (Dec. 3, 2018), https://www.theverge.com/2018/12/3/18123752/tumblr-adult-content-porn-ban-date-explicit-changes-why-safe-mode.

[11] *See* Elliot Harmon, *Facebook's Sexual Solicitation Policy is a Honeypot for Trolls*, EFF (Dec. 7, 2018), https://www.eff.org/deeplinks/2018/12/facebooks-sexual-solicitation-policy-honeypot-trolls.

D. An Unqualified Section 230(c)(2)(B) Immunity Ensures a Highly Competitive Market for Online Filtering Tools, Consistent with Congress' Goals

On the other hand, interpreting Section 230(c)(2)(B) as the plain language makes clear—that is, as creating an unqualified immunity for filtering tool providers—ensures a highly competitive market for such tools. With guaranteed immunity, many players will feel free to enter the filtering tool market, and filtering tool providers will feel free to engineer powerful products to the benefit of Internet users. Further, because these tools can produce false positives, broadly interpreting Section 230(c)(2)(B) ensures that filtering tool providers have the legal breathing room to make mistakes while striving to build better tools. This ultimately ensures that Internet users have a plethora of choices when looking for filtering tools, either for themselves or their families, workplaces, schools, libraries, and so on; it also ensures that platforms have choices so they can create online spaces for a diverse array of audiences.

The *Enigma* panel was correct that "Congress wanted to encourage the development of filtration technologies." *Enigma Software Group USA, LLC*, 938 F.3d at 1036. Unequivocal protection for filtering tool providers under Section 230(c)(2)(B) creates the market incentives consistent with Congress' stated policy goals: "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the

Internet and other interactive computer services;" and "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." *See* 47 U.S.C. § 230(b)(3) & (b)(4). *See also Enigma Software Group USA, LLC*, 938 F.3d at 1040 (Rawlinson, J., dissenting) ("The majority's policy arguments are in conflict with our recognition in *Zango* that the broad language of the Act is consistent with 'the Congressional goals for immunity' as expressed in the language of the statute.").

III. An Unqualified Section 230(c)(2)(B) Immunity Incentivizes Non-Profits Like EFF to Create Robust User-Empowerment Tools

The market incentives created by an unqualified Section 230(c)(2)(B) immunity do not apply just to for-profit companies. Non-profit, public interest organizations also benefit from a broad reading of the law, including *amicus* EFF and the partners it works with. This is evidenced by two examples.

First, EFF's team of public interest technologists has developed a free privacy-enhancing tool called Privacy Badger,[12] which is a browser add-on that was designed for Internet users who want to browse the Internet without having a third party secretly track them.[13] Privacy Badger does not use a prespecified block list,

[12] *See generally Privacy Badger*, EFF, https://www.eff.org/privacybadger.

[13] *What is Privacy Badger?*, EFF, https://www.eff.org/privacybadger/faq#What-is-Privacy-Badger.

but instead uses a heuristic to block content from domains that appear to be tracking Internet users.[14] In some cases, this can lead to preventing Internet users from seeing ads from companies that track them—potentially including ads run by entities opposed to EFF's advocacy or the views EFF espouses, or even ads run by entities providing competing privacy-enhancing software (essentially the closest thing EFF has to "competitors").[15] Thus, EFF has created a kind of filtering tool and directly benefits from the immunity provided by Section 230(c)(2)(B). Should EFF face lawsuits alleging that it has somehow acted in "bad faith" by blocking third-party trackers and the ads they serve online, EFF's ability to continue providing free privacy-enhancing tools to Internet users will be seriously threatened.

Second, EFF's Threat Lab team of cybersecurity researchers has recently been focusing on the problem of "spouseware" or "stalkerware," tracking software surreptitiously installed on someone's smartphone typically by a suspicious, paranoid, obsessed, or vindictive romantic partner.[16] These secret voyeurs are also often domestic violence perpetrators—and they use these tracking tools to terrorize

---

[14] *How does Privacy Badger work?*, EFF, https://www.eff.org/privacybadger/faq#How-does-Privacy-Badger-work.

[15] *Why does Privacy Badger block ads?*, EFF, https://www.eff.org/privacybadger/faq#Why-does-Privacy-Badger-block-ads.

[16] Rebecca Jeschke, *EFF's New "Threat Lab" Dives Deep into Surveillance Technologies—And Their Use and Abuse*, EFF (April 4, 2019), https://www.eff.org/deeplinks/2019/04/effs-new-threat-lab-dives-deep-surveillance-technologies-and-their-use-and-abuse.

their victims. Their victims often do not understand "[h]ow their abusers seem to know where they've been and sometimes even turn up at those locations to menace them," or "[h]ow they flaunt photos mysteriously obtained from the victim's phone, sometimes using them for harassment or blackmail."[17] EFF has been working to convince filtering tool companies to flag this kind of spyware, which is often marketed by the companies that develop it as legitimate.[18] Kaspersky Lab—the defendant in the *Zango* case—heeded EFF's call and "added a feature to its Android antivirus app that alerts users if their data is being tracked by known spyware."[19] Given that one of EFF's goals is to eradicate stalkerware entirely, EFF fears that providers of filtering tools will no longer cooperate with EFF's requests to block stalkerware if doing so would expose them to potential lawsuits alleging that they

[17] Andy Greenberg, *Hacker Eva Galperin Has a Plan to Eradicate Stalkerware*, Wired (April 3, 2019), https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/.

[18] *See, e.g.*, Lisa Weintraub Schifferle, *Stalking apps: Retina-X settles charges*, Federal Trade Commission (Oct. 22, 2019) (describing an FTC settlement with a stalkerware app developer that created tools that "were marketed for monitoring children and employees, but in the wrong hands, they let abusers track people's physical movements and online activities"), https://www.consumer.ftc.gov/blog/2019/10/stalking-apps-retina-x-settles-charges/.

[19] Sean Lyngaas, *Kaspersky Lab looks to combat "stalkerware" with new Android feature*, CyberScoop (April 3, 2019), https://www.cyberscoop.com/kaspersky-lab-looks-combat-stalkerware-new-android-feature/.

have somehow acted in "bad faith" by blocking these spyware products, especially if stalkerware companies claim these products are actually legitimate.

CONCLUSION

For the foregoing reasons, *amici* urge this Court to grant panel rehearing or rehearing en banc to review the panel decision in *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 938 F.3d 1026 (9th Cir. 2019).

Dated: November 6, 2019

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
sophia@eff.org
amackey@eff.org
(415) 436-9333

Attorneys for Amici Curiae Electronic Frontier Foundation and CAUCE North America, Inc.

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32, I certify as follows:

1. This Brief of *Amici Curiae* Electronic Frontier Foundation and CAUCE North America, Inc. in Support of Defendant-Appellee Malwarebytes, Inc.'s Petition for Panel Rehearing and Rehearing En Banc complies with the type-volume limitation of Fed. R. App. P. 29(b) and Cir. R. 29-2(c)(2) because this brief contains 3,739 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14-point Times New Roman font.

Dated: November 6, 2019

By: /s/ *Sophia Cope*
Sophia Cope

Counsel for Amici Curiae
Electronic Frontier Foundation and
CAUCE North America, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on November 6, 2019, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: November 6, 2019

By: /s/ *Sophia Cope*
Sophia Cope

Counsel for Amici Curiae
Electronic Frontier Foundation and
CAUCE North America, Inc.